California Consumer Privacy Act (CCPA) & Digital Advertising Webinar

Panelists:

Alan Friel, BakerHostetler, LLP
Matthew Savare, Lowenstein Sandler, LLP
Howard Waltzman, Mayer Brown, LLP

Moderator:

Michael Hahn, IAB General Counsel

Effective

January 1, 2020

August (SB 1121) amendment: delay AG enforcement until the later of 6 months from regulations or July 1, 2020, and extend rule making until no later than July 1, 2020

Who Is Regulated

Business

- For profit in CA
- Including affiliates with common branding
- $25 M; 50k; or 50%
- Collects and determines purposes and means of processing

Service providers

- “business vs. “commercial purposes”
- Third Parties

Third Parties

Impact of CCPA on Publishers

Key Questions

- Are Publishers:
  - Businesses?
  - Service Providers?
  - Third Parties?
- By allowing IBA collection, do Publishers:
  - Collect Personal Information?
  - Sell Personal Information?
  - Disclose Personal Information to a Service Provider for a Business Purpose?
  - Disclose Personal Information for a Commercial Purpose?

Publishers are Likely a Business

A publisher is a Business if it:

- Is *for profit*;
- *Collects*, or has others collect on its behalf, personal information of CA residents;
- Alone, or jointly with others, *determines the "purposes and means of the processing of consumers' personal information*; and
- Either:
  - has annual gross revenues of *$25 Million*;
  - alone or in combination, annually buys, receives for commercial purposes, sells, or shares for commercial purposes, alone or in combination the personal information of *50k or more consumers, households or devices*; or
  - derives 50% or more of annual revenues from selling consumers' personal information.

OR – is an affiliate under a common brand that does.

Service Provider?

Third Party?

Do Publishers Collect PI by Enabling Digital Advertising?

"Collect … means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior" 1798.130(e)

- First Party collection vs. Third Party collection
- Direct collection vs. receipt from third parties

Do Publishers Sell PI by Enabling Digital Advertising?

Sale: "means selling, renting, releasing, disclosing, disseminating, *making available*, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information *by the business to another business or a third party for monetary or other valuable consideration*."

No "sell" if:

- Consumer directs the transfer and recipient does not sell (unless consistent with the Act)
  - **Does this enable "opt-in"?**
- Sharing identifier to ensure opt-out
- With a Service Provider to perform a "business purpose" if
  - Explained in privacy notices
  - Service provider does not collect, sell or use other than for the business purpose
- Merger / asset sale subject to same use

A recipient is a "Service Provider" and not a "Third Party" if:

- Contract – limiting collection, use and disclosure to the "direct business relationship" and as necessary to perform the business purpose (including no "sale")
- Certification

Or do Publishers Just Disclose for a Business Purpose?

"Business Purpose" means the use of personal information *for the business' or a service provider's operational purposes*, or other notified purposes, provided that the use of the personal information shall be reasonably necessary and proportionate to achieve the operational purpose *that is compatible with the context in which the personal information was collected*. Business purposes are:

- Auditing a current interaction and concurrent transactions, e.g., counting and verifying *ad impressions*;
- *Contextual customization of ads* shown as part of the same interaction *(if no profiles or reference to user outside of the current interaction)*;
- Providing *advertising, marketing, analytics or similar services* on behalf of the business or service provider
- To improve, upgrade or enhance a business' device or service
- Fraud prevention, security, debugging, etc.

***BUT, limitations make use beyond non-IBA / ADR / analytics infeasible*.**

Implications for Publishers

Notifications

- Publisher's own practices
  - **Not just selling but sharing**
  - **“specific pieces”**
    - Pass-through notices for others?
  - **Including notice of further sale and opt-out (1798115(d))**

Opt-in for under 16 if third party IBA collection is a sale.

Do Not Sell

- Publisher's own practices
  - ***If allowing third party IBA collection is a sale, how does the publisher stop that collection upon a do not sell request?***
  - ***Or, does it even have to under 1798.135(a)(4)?***
  - ***How does the publisher authenticate?***
    - Pass-through request mechanism for others?

Delete

Provide Copies of PI

No Discrimination (1798.125)

Impact of CCPA on Advertisers

Key Questions

- Are Advertisers:
  - Businesses?
  - Service Providers?
  - Third Parties?
- In having IBA ads served are Advertisers:
  - Collecting Personal Information?
  - Selling Personal Information?
  - Disclosing Personal Information to A Service Provider for a Business Purpose?
  - Disclosing Personal Information to a Third Party for a Commercial Purpose?

Advertisers are Likely a Business

A publisher is a Business if it:

- Is *for profit*;
- *Collects*, or has others collect on its behalf, personal information of CA residents;
- Alone, or jointly with others, *determines the "purposes and means of the processing of consumers' personal information*; and
- Either:
  - has annual gross revenues of *$25 Million*;
  - alone or in combination, annually buys, receives for commercial purposes, sells, or shares for commercial purposes, alone or in combination the personal information of *50k or more consumers, households or devices*; or
  - derives 50% or more of annual revenues from selling consumers' personal information.

OR – is an affiliate under a common brand that does.

Service Provider?

Third Party?

Do Advertisers Collect PI?

"Collect … means buying, renting, gathering, *obtaining*, *receiving*, or accessing any personal information pertaining to a consumer *by any means*. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior" 1798.130(e)

Do Advertisers Sell PI?

Sale: "means selling, renting, releasing, disclosing, disseminating, *making available*, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information *by the business to another business or a third party for monetary or other valuable consideration*."

No "sell" if:

- Consumer directs the transfer and recipient does not sell (unless consistent with the Act)
  - **Does this enable "opt-in"?**
- Sharing identifier to ensure opt-out
- With a Service Provider to perform a "business purpose" if
  - Explained in privacy notices
  - Service provider does not collect, sell or use other than for the business purpose
- Merger / asset sale subject to same use

A recipient is a "Service Provider" and not a "Third Party" if:

- Contract – limiting collection, use and disclosure to the "direct business relationship" and as necessary to perform the business purpose (including no "sale")
- Certification

Or do Advertisers Just Disclose for a Business Purpose?

"Business Purpose" means the use of personal information *for the business' or a service provider's operational purposes*, or other notified purposes, provided that the use of the personal information shall be reasonably necessary and proportionate to achieve the operational purpose *that is compatible with the context in which the personal information was collected*. Business purposes are:

- Auditing a current interaction and concurrent transactions, e.g., counting and verifying *ad impressions*;
- *Contextual customization of ads* shown as part of the same interaction *(if no profiles or reference to user outside of the current interaction)*;
- Providing *advertising, marketing, analytics or similar services* on behalf of the business or service provider
- To improve, upgrade or enhance a business' device or service
- Fraud prevention, security, debugging, etc.

BUT, the required contractual limitations make use beyond ADR infeasible

Implications for Advertisers

Notifications

- Before collection and of opt-out
  - **On Ad icon?**

Do Not Sell

- Would be business-wide not just IBA
- How to authenticate?
- How to tie back to CRM?
- Toll free number / link to radio button on website

Deletion

- Must pass through to Service Providers
- The 105(d) exceptions seem less applicable to advertisers as to publishers, excepting the free speech exception

Impact of CCPA on Intermediaries

Key Definitional Issues

1798.140

- (a) – Aggregate Consumer Information
- (c) – Business
- (d) – Business Purpose
- (e) – Collect
- (h) – Deidentified
- (o) – Personal Information
- (r) – Pseudonymize
- (t) – Sell
- (v) – Service Provider
- (w) – Third Party
- (y) – Verifiable Consumer Request

Key Questions

- How are we defining intermediaries in this presentation?
  - SSP, DSP, ad network, ad exchange, DMP, trading desks, etc.
- Are intermediaries:
  - Businesses?
  - Service Providers?
  - Third Parties?
- Do intermediaries:
  - Collect Personal Information?
  - Sell Personal Information?
  - Disclose Personal Information for a Business Purpose?

Is an Intermediary a “Business?”

- To be a “Business,” a company needs to determine the “purpose and means” of processing of consumers’ Personal Information.
- This is analogous to a data controller under the GDPR.
- Unlike the GDPR and the EU Directive, there is no supplementary CCPA guidance on what “purpose and means” is.
  - See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
  - Established case law in the EU regarding meaning of “purpose and means.”
- Intermediaries will likely look to how they designated themselves under the GDPR to determine this.

Is an Intermediary a “Service Provider?”

- If the intermediary has deemed itself a processor under the GDPR, the closest related concept under the CCPA is a “Service Provider.”
- However the definition is unclear.
- A Service Provider “processes personal information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract” provided that the contract prohibits the entity from using the data for anything other than performing specified services for the business.

Key Question re: Service Provider Status

- Does this mean that an organization can only be a Service Provider if it receives the Personal Information from the Business? Or can it collect the Personal Information from consumers directly on behalf of the Business?
  - **Based on the notice obligations, it seems like a Service Provider is meant to only receive Personal Information from the Business itself (see 1798.115).**
  - **If that is true, certain intermediaries, such as agencies, SSPs, and DMPs, may not be Service Providers depending on their particular business model; they often collect data directly from consumers on behalf of a Business.**

Key Question re: Service Provider Status

- What happens if the contract between the business and the intermediary allows the intermediary to use the data beyond merely providing services for the Business?
- Does that make the intermediary a “Business?”
- Most contracts involving intermediaries allow the intermediary to use data in an aggregated and/or anonymized fashion.
- Does that make the intermediary a “Business?”
    - Recommendation is for the contract to specify that the intermediary may aggregate and anonymize data on behalf of the Business, in which case the intermediary would likely not be considered a Business.

Is an Intermediary a “Third Party?”

- If the intermediary is not a “Business” or a “Service Provider,” then it is a Third Party.
- A third party cannot sell Personal Information it has been sold from a Business unless the Business has published an opt-out notice and the consumer has the opportunity to opt out (see 1798.115(d)).
- But what if the Third Party received the data from a Service Provider? There is no obligation for the Service Provider to enter into a contract with the Third Party to ensure the Third Party does not sell the data.

Summation on Status of Intermediaries

- Depending on the facts, intermediaries are likely Service Providers or Third Parties under CCPA.
  - An SSP is likely a Service Provider to publishers.
  - A DSP is likely a Service Provider to advertisers/agencies.
  - An ad exchange is likely a Service Provider to publishers **and** advertisers/agencies.
- However, if the intermediary controls the “purpose and means” of the data processing, it is a Business if it meets the other criteria described earlier.
  - An ad network may service as a Business.
    - Creation and sale of audience segments on behalf of various publishers, but often controls the data processing activities.

Types of Data for Intermediaries

Bid Request Data (or "bidstream data"): An advertising bid request in a specified format, such as oRTB (e.g., adID, DealID, cookie ID, geolocation, website/app, user agent string, device type, carrier name, campaign ID).

- Often sent by from a user device to an ad exchange or SSP to facilitate programmatic advertising

Header Information (or "clickstream data"): The end-user's 'journey' on a website or app collected by a server (e.g., IP address, referring URL, exit URL, actions taken, cookie preferences, device information)

- Often collected by third-party ad servers and DMPs

Event Data (or "conversion data"): Pre-defined actions that a party wants an end-user to take, usually after clicking on an ad (e.g., add to shopping cart, purchase, app install, form submission).

- Often collected by DMPs, retargeters, and analytics providers.

Cross-Device Data (or "Device Graph Data"): Data that displays the relationship between various device identifiers to an individual or household, often used for better retargeting and frequency capping.

- Often collected by DSPs and SSPs through cookie syncing.

What is Triggered If a Business "Collects" Personal Information?

1798.100 – Notice and Access Requirements

- (b) – Collection of Personal Information triggers the notice requirements in 1798.100(b) and if a Business receives a Verifiable Consumer Request, Business must provide consumer access to the Personal Information pursuant to 1798.100(d).
- Key Takeaways
  - Intermediaries clearly "Collect" Personal Information:
    - **"Collection" concerns obtaining information "pertaining" to a consumer, not necessarily from a consumer.**
    - **As noted, "Personal Information" is defined incredibly broadly.**
- Key Query
  - Does 1798.100(e) create a loophole for one-time transactions?
  - Similar to the GDPR, Businesses only need to fulfill "Verifiable Consumer Requests." In other words, Businesses do not need to fulfill requests if they cannot "verify" the person making the request. In the world of AdTech, much Personal Information is predicated upon randomized user IDs (a random string of characters) and is not associated directly with a name or email address. So, this might also be a big carve-out for intermediaries that may need to assist with, or be directly accountable for, a consumer request.

What is Triggered If a Business "Collects" Personal Information?

1798.105 – Notice and Deletion Requirement

- (b) – Business needs to disclose consumer's right to request deletion of any Personal Information.
- (c) – If company receives verifiable request, it must delete the Personal Information and direct any Service Provider to delete the Personal Information.
- Key Takeaways
  - If intermediary is a Service Provider, it must delete Personal Information if requested by Business.
- Key Query:
  - Do any of the exceptions to the deletion requirement in 1798.105(d), which apply to Businesses and Service Providers, apply to intermediaries?
    - **The "internal use" exceptions in (d)(7) and (d)(9) may apply in a walled garden environment, but probably not for intermediaries.**

What is Triggered If a Business "Sells" Personal Information or Discloses It for a "Business Purpose?"

1798.115 – Notice and Disclosure Requirement

- (b) – Requires Business to provide information described in (a) upon receipt of Verifiable Consumer Request.
- (c) – Requires certain disclosures in privacy policy.
- (d) – Provides consumer an opt out right if Personal Information is "Sold" to a Third Party and such Third Party seeks to "Sell" the Personal Information.
  - Note – no opt out right for disclosure of Personal Information for a "Business Purpose."
  - Note – does not seem to apply to Service Providers.
- Key Takeaways
  - Very broad definition of "Sell" (i.e., for money or other valuable consideration")
    - **Most intermediaries presumably "Sell" Personal Information.**
  - Of the intermediaries that do not "Sell" Personal Information, they almost certainly disclose it for Business Purposes.
    - **See 1798(d)(1), (2), (4), and (5) – counting ad impressions to unique visitors, verifying impressions, detecting fraud, contextual ads, "providing advertising or marketing services."**

What is Triggered If a Business "Sells" Personal Information or Discloses It for a "Business Purpose?"

1798.120 – Opt Out Right

- (a) – Provides consumer an opt out right to prevent a Business from selling the Personal Information to a Third Party.
  - Note – Again, no opt right for "Disclosure" of Personal Information for a "Business Purpose."
- (b) – Requires notice in the Business' privacy policy that it "Sells" Personal Information Third Parties.
- (d) – Expands COPPA-type opt-in protections for 13, 14, and 15 year olds.

What is Triggered If a Business "Sells" Personal Information or Discloses It for a "Business Purpose?"

1798.135 – Do Not Sell

- (a) – Any Business that is required to provide consumers the ability to opt out under 1798.120 is required to provide a "clear and conspicuous link" on its homepage (or a CA-specific page to which CA consumers are directed) that directs the consumer to a "Do Not Sell My Personal Information" page.

No Consent Concept for Sale of Personal Data

- A Business does not sell Personal Information to a Third Party if the consumer "intentionally interacts with a third party" and the Third Party does not also sell the Personal Information. See 1798.140(t)(2)(A).
- Unlike the GDPR, the standard for consent is not fleshed out in the CCPA.
- What does "intentionally interact" mean? If the consumer opts-in to cookies, is that an intentional interaction with each Third Party cookie provider?
- If the consumer clicks on an ad served by a Third Party, is that an intentional interaction for all uses of Personal Information in relation to such ad?

Exemption for Deidentified or Aggregate Consumer Information

1798.145(a)(5)

- The statute does not restrict a company's ability to: "Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information."
- Key Queries
  - How broad is this exemption?

Appendix

Who Is Protected

- **"Consumers," defined as California residents, determined by tax payer status, includes:**
  - **individuals in the State for other than a temporary or transitory purpose; and**
  - **individuals domiciled in the State but outside the State for a temporary or transitory purpose,**

  however identified, including by any unique identifier.

- **Consumers include, but are not limited to, customers of household goods and services, a departure from other California privacy laws.**
- **Thus employees are covered, as are B-to-B transactions.**

Children

- **Opt-in for selling PI:**
  - of minor aged 13 – 16;
  - by parent for children under 13.
  - Willful disregard of age = knowledge

What Data

- **“Personal Information” is information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Consumer or household.**
- **Personal information may include, but is not limited to, 11 categories (which categories must be used when providing required notices and disclosures).**
    - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

What Data

- Traditional PII: Signature, physical characteristics or description, address, telephone number, state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
- Characteristics of protected classifications under California or federal law (e.g., race, gender, sexual orientation, etc.).
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.

What Data

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a Consumer's interaction with an Internet website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- Inferences drawn from any of the information identified in this subdivision to create a profile about a Consumer reflecting the Consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

What Data

- Excludes “publicly available” information from public government records, but explicitly does not include, biometric data collected without the Consumer’s knowledge and data used for an incompatible purpose as publicly available.
- Carve outs for protected health information governed by CA and federal health information privacy laws and to a lesser degree data regulated by certain other CA and federal privacy laws (e.g., Gramm-Leach-Bliley for financial institutions).
- Unclear whether pseudonymous data, deidentified data, and aggregate data are considered “personal information,” but such data is excluded from the restrictions on collection, use, retention, sale and disclosure.

Pre-collection Privacy Notice Requirements

- **A Business must track personal information collected, and inform Consumers at or before collection, in a form reasonably available:**
  - the categories of personal information collected; and
  - the purposes (business purposes and commercial purposes) for the collection of each category
- **Limit the use to those purposes absent further advance notice.**
- **A description of Consumers' rights under the CCPA**

Online Privacy Notice Requirements

- A list of categories of personal information collected in the preceding 12 months and the purposes (business purposes and commercial purposes) therefore – use of another purpose requires further notice prior to different use;
- If it sells personal information, that personal information may be sold and how to opt-out of the sale of personal information;
- A list of the categories of personal information sold in the preceding 12 months;
- A list of the categories of personal information disclosed for a business purpose in the preceding 12 months;
- Any financial incentives for providing data or not exercising rights.

Privacy Notice Requirements

- **Third Parties, even if not a Business, need to give, or have the Business give, Consumers explicit notice and an opportunity to opt out prior to re-selling their personal information that was sold to the Third Party by a Business.**
- **Does this include M&A successors? They at least have to give notice and opt-out before different use.**

Request Rights

- **If verified:**
  - To request disclosure, including specifics of a particular Consumer's PI
  - To obtain portable copies of PI
  - To delete PI information
    - which may be limited to only the information the Business has collected, and is subject to limited exceptions
    - businesses must require their Service Providers also delete personal information upon a Consumer request to the Business
      - **but due to the definition of Service Provider this does not apply to vendors engaged for commercial purposes**
- **"Do not sell"**
  - No verification obligation, so identifier would seem to be enough to qualify

Request Rights

Upon a verified request from the Consumer, a Business must provide the following information to the Consumer on an individualized basis (i.e., specific to his or her data):

- the categories of personal information collected about that specific Consumer;
- the categories of sources from which the personal information is collected;
- the specific pieces of personal information collected about that Consumer;
- the business purpose(s) and commercial purpose(s) for collecting or selling the PI;

Request Rights

- the categories of Third Parties (which includes differently branded affiliates, and possibly similarly branded affiliates, but does not include Service Providers engaged for business purposes if certain requirements are met, but does include vendors for commercial purposes) with which the business “shares” PI;
- for PI disclosed for a business purpose, the categories of the Consumer’s PI disclosed. There is no obligation to include in an information request response information on PI disclosed for commercial purposes that are not a sale, though that may be added before the effective date and it is suggested that this also be provided; and
- for PI that is sold, the categories of the Consumer’s PI sold and for each category to what categories of Third Parties

Responding to Rights Requests

- **Must verify the Consumer making a request (portability, deletion or information; not DNS)**
  - Pursuant to regs
- **Most requests limited to twice a year and to a 12-month look-back, but no limits on deletion and do not sell requests**
- **Typically 45 days**
- **Ordinarily free**
- **Cannot require account registration**
- **May limit retention and don’t have to re-identify**

The Opt-out Request

- “Do Not Sell” link and other mechanism – toll-free number
- What is a sale?
- May use an agent
- Details of process to be in regs
- No solicitation of opt-in or withdraw of opt-out for 12 months
- Various exceptions apply